

Remarks

The Office Action mailed January 4, 2007, has been carefully reviewed and the foregoing amendment has been made in consequence thereof.

Applicant believes that no extension of term is required and that no additional fee for claims is required. If any additional fee is required for an extension of term or claims, the Commissioner is hereby authorized to charge Deposit Account No. 01-2384.

Claims 13-40 and 46-48 are now pending in this application. Claims 13-40 and 46-48 stand rejected. Claims 1-12 and 41-45 have been cancelled.

The objection to Claims 13 and 21 due to an informality is respectfully traversed. Claims 13 and 21 have been amended according to the suggestions in the Office Action. For the reasons set forth above, Applicants request that the objection to Claims 13 and 21 be withdrawn.

The rejection of Claims 13 and 34 under 35 U.S.C. § 112, first paragraph, and the objection to the specification, are respectfully traversed. Claims 13 and 34 have been amended to address the issues noted in the Office Action. For the reasons set forth above, Applicants respectfully request that the Section 112 rejections of Claims 13 and 34, and the objection to the specification, be withdrawn.

The rejection of Claims 13-40 and 46-48 under 35 U.S.C. § 103 as being unpatentable over Jonstromer (6,142,369) in view of Falk et al. (5,668,876) is respectfully traversed.

While Jonstromer is related to electronic transactions, nothing in Column 1, lines 7-44, describe a signing unit or the digital signing of a message to be transmitted. Rather, Jonstromer describes use of a stored value card and a subscriber information module (SIM) which allows a user to use (access) a mobile phone once the SIM is inserted into the phone and a Pin is entered. The SIM may include encryption algorithms and keys, but there is no description of message signing. Column 1, lines 10-13 of Jonstromer describe electronic credits stored on a smart card, not a signed message.

More specifically, Jonstromer describes an electronic transaction system for conducting electronic financial transactions including a smart card configured to store a plurality of payer electronic credits and a communication module configured to transmit the electronic credits from the smart card to a party selected from a plurality of addressable parties accessible through a Public Switched Telephone Network. See Abstract. Referring to Column 3, lines 50-59, Jonstromer describes that a communications module transmits a signal indicating an amount to be transferred, an address of a payee, an account number and an electronic signature of a payer to an electronic banking terminal at the bank. Further, the electronic banking terminal authenticates the electronic signature, debits the account of the payer and credits the account of the payee, and the electronic banking terminal transmits a signal to the electronic till of the payee confirming payment.

At Column 4, lines 38-52 Jonstromer states the signal transmitted by mobile telephone 4, to electronic till 2, may include an electronic signature encoded by means of an asymmetric cypher and key, which uniquely and securely identifies the smart card. Access to use of the smart card is controlled by use of a PIN (personal identity number) known only to the owner of the smart card. Further, all signals transmitted between the mobile phone 4, and the electronic till 2, are securely encrypted using the RSA authentication system (Rivest, Shamir and Adleman public key encryption system). This system may be used both for encryption and provision of a secure electronic signature. While Jonstromer describes an electronic signature, and encryption using public keys, it does not describe the signing of a message via a mobile telephone. Specifically, Jonstromer does not describe transmitting a message to be signed, the signing of the message, and the subsequent retransmission of the signed message as recited in Claim 13. Further, Jonstromer only describe transmission of signed messages originating from the mobile telephone 4.

Falk et al. describe a personal unit that includes a receiver for receiving a transmitted challenge code and an algorithm unit which processes the challenge code, a user input such as a personal identification number (PIN) or electronically recognizable signature, and an internally stored security key for calculating a response code according to a pre-stored algorithm. The

response code is then sent to the service node and, if it is acceptable, access to the service is authorized. A method associated with Falk et al. involves receiving a challenge code from a system, the user inputting a personal identification number or other recognizable input, and the personal unit generating a response code based on an internally stored algorithm. The challenge code and the response is unique for each transaction. See Column 2, lines 6-21.

Now referring to Column 2, line 67 to Column 3, line 14, Falk et al. describe a personal unit 20 for generating a response code, a terminal 22 for initiating service access and conducting service, and for inputting the response code to a service access network 24. The service access network transmits data between the terminal 22 and a service node 26. The service node 26 generates a challenge code and requests that the challenge code be sent to the personal unit 20 via an authentication challenge network 28. Alternatively, the separate authentication center 30 can generate the challenge code upon request by the service node 26. The terminal 22 can be a land-line telephone, a radio telephone, an ATM, a computer with a modem (modulator/demodulator), a facsimile machine, or virtually any other type of terminal capable of receiving an input directly or indirectly from the personal unit 20 and relaying information to a service node 26.

Claim 13 recites a method for digital signing of a message which is transmitted via a communication network to a signing unit. The method includes “transmitting from a transmitter a message to be signed to a first receiver”, transmitting the message to be signed from the first receiver via a telephone network to a mobile radio telephone comprising a signing unit, the telephone network comprising a mobile radio telephone network, the mobile radio telephone associated with the telephone network”, “signing the message to be signed via the mobile radio telephone, thereby forming a signed message, the signed message signifying a user’s intent to deliver the signed message and its content”, “transmitting the signed message to the first receiver or at least one other receiver” and “communicating the signed message to an addressee.”

Jonstromer in view of Falk et al. do not describe or suggest the claimed combination. Jonstromer describes an electronic signature, and encryption using public keys, it does not describe the signing of a message via a mobile telephone. Specifically, Jonstromer does not

describe transmitting a message to be signed, the signing of the message, and the subsequent transmission of the signed message. Falk et al. also do not describe transmitting a message to be signed to a first receiver. Rather, Falk et al. variously describe transmission of an account number, a challenge code, and a challenge response code. Nowhere do Falk et al. describe a message to be signed or a signed message. In contrast to Claim 13, Falk et al. merely describe receipt of a challenge code and generating response to the challenge. However, the response to the challenge is not properly construed as being a signed message.

Further, Jonstromer and Falk et al. appear to teach away from one another, and therefore, their combination. Specifically, Jonstromer describes public key encryption and Falk et al. describe challenge and response codes. While encryption, challenges, and response codes are related, they are not fairly characterized as a message to be signed and a signed message.

For the reasons set forth above, Claim 13 is submitted to be patentable over Jonstromer in view of Falk et al.

Claims 14-20 depend, directly or indirectly, from independent Claim 13. When the recitations of Claims 14-20 are considered in combination with the recitations of Claim 13, Applicants submit that dependent Claims 14-20 likewise are patentable over Jonstromer in view of Falk et al.

Claim 21 recites a signed message created by the process of Claim 13. As described above, Jonstromer in view of Falk et al. do not describe, nor suggest, a transmitter transmitting a message to be signed to a receiver, which then transmits the message to be signed from the receiver to a mobile radio telephone that includes a signing unit. Therefore neither of Jonstromer and Falk et al. describe or suggest a transmitter transmitted a message to be signed to a receiver, nor a receiver that transmits the message to be signed to a mobile radio telephone that includes a signing unit, which provides a signed message. Rather and as described above, Jonstromer describes public key encryption and Falk et al. describe challenge and response codes.

For the reasons set forth above, Claim 21 is submitted to be patentable over Jonstromer in view of Falk et al.

Claim 22 recites a method for digitally signing, by means of a signing apparatus, a message to be transmitted to a receiving device. The message to be signed is transmitted from a transmitting device to a receiving device, this message is then transmitted from the receiving device via a telephone network to a signing apparatus associated with the transmitting device. The message is then signed in the signing apparatus and transmitted back to the receiving device as a signed message.

Jonstromer in view of Falk et al. do not describe nor suggest a method that includes transmitting a message to be signed from a transmitting device to a receiving device, where this message is then transmitted from the receiving device via a telephone network to a signing apparatus associated with the transmitting device. Rather, Jonstromer describes a communications module that transmits a signal indicating at least an electronic signature of a payer to an electronic banking terminal at the bank. Jonstromer do not describe transmission of a non-signed message (e.g., a message to be signed).

More specifically, Jonstromer states the signal transmitted by mobile telephone 4, to electronic till 2, may include an electronic signature encoded by means of an asymmetric cypher and key, which uniquely and securely identifies the smart card. Access to use of the smart card is controlled by use of a PIN (personal identity number) known only to the owner of the smart card. The system of Jonstromer may be used both for encryption and provision of a secure electronic signature. While Jonstromer describes an electronic signature, and encryption using public keys, it does not describe the signing of a message via a mobile telephone. Specifically, Jonstromer does not describe transmitting a message to be signed from a transmitter to a signing apparatus utilizing a receiving device as described by Claim 22, nor does Jonstromer describe the signing of the message, and the subsequent transmission of the signed message as recited in Claim 22.

Falk et al. variously describe transmission of an account number, a challenge code, and a challenge response code. Nowhere do Falk et al. describe transmitting a message to be signed, signing the message, or a transmission of the signed message. More specifically, Falk et al. does not describe a transmitter transmitting a message to be signed to a receiver, which then transmits the message to be signed from the receiver to a mobile radio telephone that includes a signing unit.

For the reasons set forth above, Claim 22 is submitted to be patentable over Jonstromer in view of Falk et al.

Claims 23-32 depend, directly or indirectly, from independent Claim 22. When the recitations of Claims 23-32 are considered in combination with the recitations of Claim 22, Applicants submit that dependent Claims 23-32 likewise are patentable over Jonstromer in view of Falk et al..

Independent Claim 33 recites a chip card for a mobile telephone, wherein the chip card incorporates a signing device which has a memory unit for storing a private key necessary for producing a signed message. The signing device generates the signed message from a message to be signed which is received by the mobile telephone via a telephone network.

Jonstromer in view of Falk et al. do not describe nor suggest a chip card for a mobile telephone that includes a signing device that generates a signed message from a message to be signed that was received by the mobile telephone. Rather, Jonstromer describes a communications module that transmits a signal indicating at least an electronic signature of a payer to an electronic banking terminal at the bank.

More specifically, Jonstromer states the signal transmitted by mobile telephone 4, to electronic till 2, may include an electronic signature encoded by means of an asymmetric cypher and key, which uniquely and securely identifies the smart card. Access to use of the smart card is controlled by use of a PIN (personal identity number) known only to the owner of the smart card. The system of Jonstromer may be used both for encryption and provision of a secure

electronic signature. While Jonstromer describes an electronic signature, and encryption using public keys, it does not describe a chip card for a mobile telephone that includes a signing device that generates a signed message from a message to be signed that was received by the mobile telephone.

Falk et al. variously describe transmission of an account number, a challenge code, and a challenge response code. Nowhere do Falk et al. describe a signing device that generates a signed message from a message to be signed which is received by the mobile telephone via a telephone network.

For the reasons set forth above, Claim 33 is submitted to be patentable over Jonstromer in view of Falk et al.

Independent Claim 34 recites a method for transport via a communication network of a message to a mobile phone and transport of a corresponding signed message. The method comprises “transmitting from a transmitter a message to be signed to a first receiver” and “transmitting the message to be signed from the receiver via a telephone network to a mobile radio telephone whereat the message to be signed may be signed, and when signed, generates a corresponding signed message.”

Jonstromer describes an electronic signature, and encryption using public keys, it does not describe the signing of a message via a mobile telephone. Specifically, Jonstromer does not describe transmitting from a transmitter a message to be signed to a first receiver and transmitting the message to be signed from the receiver via a telephone network to a mobile radio telephone whereat the message to be signed may be signed, and when signed, generates a corresponding signed message. Jonstromer, as best understood, only relates to transmission of previously signed messages. Falk et al. also do not describe transmitting a message to be signed to a first receiver. Rather, Falk et al. variously describe transmission of an account number, a challenge code, and a challenge response code. Nowhere do Falk et al. describe a message to be signed or a signed message or transmitting the message to be signed from the receiver via a telephone network to a mobile radio telephone.

For the reasons set forth above, Claim 34 is submitted to be patentable over Jonstromer in view of Falk et al..

Claims 35-38 depend, directly or indirectly, from independent Claim 34. When the recitations of Claims 35-38 are considered in combination with the recitations of Claim 34, Applicants submit that dependent Claims 35-38 likewise are patentable over Jonstromer in view of Falk et al..

Claim 39 recites a method, comprising “a mobile radio telephone user receiving a message from a telephone network” and “the user using the mobile radio telephone to generate a signed message corresponding to the received message...”.

Jonstromer in view of Falk et al. do not describe nor suggest a method that includes receiving a message from a telephone network and the user using the mobile radio telephone to generate a signed message corresponding to the received message. Rather, Jonstromer describes a communications module that transmits a signal that includes at least an electronic signature of a payer to an electronic banking terminal at the bank. As such, Jonstromer does not describe receiving a message from telephone network that is to be signed.

More specifically, Jonstromer states the signal transmitted by mobile telephone 4, to electronic till 2, may include an electronic signature encoded by means of an asymmetric cypher and key, which uniquely and securely identifies the smart card. Access to use of the smart card is controlled by use of a PIN (personal identity number) known only to the owner of the smart card. The system of Jonstromer may be used both for encryption and provision of a secure electronic signature. While Jonstromer describes an electronic signature, and encryption using public keys, it does not describe the signing of a message via a mobile telephone.

Falk et al. variously describe transmission of an account number, a challenge code, and a challenge response code. Nowhere do Falk et al. describe transmitting a message to be signed, signing the message, or a transmission of the signed message. More specifically, Falk et al. do not describe using the mobile radio telephone to generate a signed message corresponding to the

received message. As such, generation of a signed message corresponding to a received message is not described in either of Jonstromer and Falk et al.

For the reasons set forth above, Claim 39 is submitted to be patentable over Jonstromer in view of Falk et al.

Claim 40 depends from independent Claim 39. When the recitations of Claim 40 are considered in combination with the recitations of Claim 39, Applicants submit that dependent Claim 40 likewise is patentable over Jonstromer in view of Falk et al.

Claim 46 recites a wireless device for receiving a message to be signed and transmitting a corresponding signed message. The device includes input apparatus for accepting input from a user indicating the received message is to be signed and memory for storing an algorithm for generating a corresponding signed message.

Jonstromer in view of Falk et al. do not describe nor suggest a wireless device for receiving a message to be signed and transmitting a corresponding signed message that includes input apparatus for accepting input from a user indicating the received message is to be signed and memory for storing an algorithm for generating a corresponding signed message. Rather, Jonstromer describes a communications module that transmits a signal indicating at least an electronic signature of a payer to an electronic banking terminal at the bank.

More specifically, Jonstromer states the signal transmitted by mobile telephone 4, to electronic till 2, may include an electronic signature encoded by means of an asymmetric cypher and key, which uniquely and securely identifies the smart card. Access to use of the smart card is controlled by use of a PIN (personal identity number) known only to the owner of the smart card. The system of Jonstromer may be used both for encryption and provision of a secure electronic signature. While Jonstromer describes an electronic signature, and encryption using public keys, it does not describe a wireless device for receiving a message to be signed and the subsequent transmission of a corresponding, signed message.

Falk et al. variously describe transmission of an account number, a challenge code, and a challenge response code. Nowhere do Falk et al. describe transmitting a message to be signed, signing the message, or a transmission of the signed message. More specifically, Falk et al. do not describe a device that includes input apparatus for accepting input from a user indicating the received message is to be signed and memory for storing an algorithm for generating a corresponding signed message.

For the reasons set forth above, Claim 46 is submitted to be patentable over Jonstromer in view of Falk et al.

Claims 47-48 depend, directly or indirectly, from independent Claim 46. When the recitations of Claims 47-48 are considered in combination with the recitations of Claim 46, Applicants submit that dependent Claims 47-48 likewise are patentable over Jonstromer in view of Falk et al.

For the reasons set forth above, Applicants respectfully request that the Section 103 rejection of Claims 13-40 and 46-48 be withdrawn.

In addition to the reasons given above, Applicants respectfully submit that the Section 103 rejection of the presently pending claims is not a proper rejection. As is well established, obviousness cannot be established by combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. No combination of Jonstromer and Falk et al. describes or suggests the claimed combination. Furthermore, in contrast to the assertion within the Office Action, Applicants respectfully submit that it would not be obvious to one skilled in the art to combine Jonstromer with Falk et al. because there is no motivation to combine the references suggested in the art. Additionally, the Examiner has not pointed to any prior art that teaches or suggests to combine the disclosures, other than Applicants' own teaching. Rather, only the conclusory statement along the lines that "it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of transmitting from a transmitter a message to be signed to a first receiver and transmitting the message to be signed from the receiver via a telephone network to a mobile

radio telephone, the telephone network comprising a mobile radio telephone network in the system of Jonstromer, as Falk teaches, so as to provide secure electronic services such as banking services” suggests combining the disclosures.

As the Federal Circuit has recognized, obviousness is not established merely by combining references having different individual elements of pending claims. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP 2143.01. Rather, there must be some suggestion, outside of Applicants’ disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicants’ disclosure. In re Vaeck, 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case, neither a suggestion or motivation to combine the prior art disclosures, nor any reasonable expectation of success has been shown.

Moreover, as is well established, the mere fact that the prior art structure could be modified does not make such a modification obvious unless the prior art suggests the desirability of doing so. *See In re Gordon*, 221 U.S.P.Q.2d 1125 (Fed. Cir. 1984). Furthermore, the Federal Circuit has determined that:

[i]t is impermissible to use the claimed invention as an instruction manual or “template” to piece together the teachings of the prior art so that the claimed invention is rendered obvious. This court has previously stated that “[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention.”

In re Fitch, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992).

Further, under Section 103, “it is impermissible...to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.” In re Wesslau, 147 USPQ 391, 393 (CCPA 1965). Rather, there must be some suggestion, outside of Applicants’ disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicants’ disclosure. In re Vaeck, 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case,

neither a suggestion nor motivation to combine the cited art, nor any reasonable expectation of success has been shown. Accordingly, since there is no teaching nor suggestion in the cited art for the claimed combination, the Section 103 rejection appears to be based on a hindsight reconstruction in which isolated disclosures have been picked and chosen in an attempt to deprecate the present invention. Of course, such a combination is impermissible, and for this reason, along with the reason provided previously, Applicants request that the Section 103 rejection of Claims 13-40 and 46-48 be withdrawn.

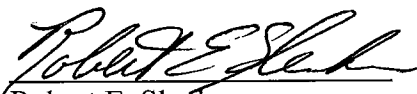
Moreover, if art “teaches away” from a claimed invention, such a teaching supports the nonobviousness of the invention. U.S. v. Adams, 148 USPQ 479 (1966); Gillette Co. v. S.C. Johnson & Son, Inc., 16 USPQ2d 1923, 1927 (Fed. Cir. 1990). In light of this standard, it is respectfully submitted that the cited art, as a whole, is not suggestive of the presently claimed invention. Specifically, Applicants respectfully submit that Falk et al. and Jonstromer teach away from the present invention, and as such, there is no suggestion or motivation to combine Jonstromer with Falk et al.. Specifically, in contrast to the present invention, Jonstromer describes a communications module that transmits a signal indicating the amount to be transferred, the address of the payee, the account number, and an electronic signature of the payor, based on public key encryption, to an electronic banking terminal at the bank, and in contrast to Jonstromer and the present invention, Falk et al. describe a personal unit that includes a receiver for receiving a transmitted challenge code and an algorithm unit which processes the challenge code, a user input such as a personal identification number (PIN) or electronically recognizable signature, and an internally stored security key for calculating a response code according to a pre-stored algorithm.

More specifically, no combination of Jonstromer and Falk et al. describes or suggests an apparatus or method that includes transmitting a message to be signed to a receiver, signing the message to generate a corresponding signed message, and transmitting the corresponding signed message to one or more receivers. Accordingly, Jonstromer and Falk et al. teach away from the present invention, and from each other, and as such, any combination of the cited art appears to

support the non-obviousness of the present invention. Accordingly, Claims 13-40 and 46-48 are submitted to be patentable over Jonstromer in view of Falk et al.

In view of the foregoing amendments and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,

A handwritten signature in cursive script, appearing to read "Robert E. Slenker", written in dark ink.

Robert E. Slenker
Registration No. 45,112
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070